

FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ALEXANDER MONTAGU HAY,

Defendant-Appellant.

No. 99-30101

D.C. No.

CR-98-00340-BJR

OPINION

Appeal from the United States District Court
for the Western District of Washington
Barbara J. Rothstein, Chief District Judge Presiding

Argued and Submitted
May 3, 2000--Seattle, Washington

Filed October 24, 2000

Before: Pamela Ann Rymer and Thomas G. Nelson,
Circuit Judges, and James R. Browning, District Judge.*

Opinion by Judge Rymer

*Honorable William D. Browning, United States District Judge for the
District of Arizona, sitting by designation.

COUNSEL

Jonathan S. Solovy, Bell, Flegenheimer & Solovy, Seattle, Washington, for the defendant-appellant.

Floyd G. Short, Assistant United States Attorney, Seattle, Washington, for the plaintiff-appellee.

OPINION

RYMER, Circuit Judge:

Alexander Hay appeals his conviction following a jury trial for possession and distribution of child pornography by means of a computer. Hay contends that the search of his entire computer system based on a seven-minute, six-month old transmission of 19 images of child pornography was unreasonable; he faults the district court for allowing the jury to view three

13392

exhibits containing child pornography; and he submits that his conviction is invalid under our recent decision in Free Speech Coalition v. Reno, 198 F.3d 1083 (9th Cir. 1999). We disagree, and affirm.

I

Dr. Blair Evans was arrested on November 29, 1996 in Ontario, Canada for trafficking in child pornography. He had more than 20,000 computer graphic images of child pornography and was actively trading and exchanging child pornography with individuals in the United States through the Internet. According to the File Transfer Protocol (FTP)² log in Evans's computer, two days before his arrest he transmitted 19 graphics files (including images depicting an adult male and a pre-pubescent girl of about five years engaging in sexual conduct) from his computer to a computer with the Internet address of

128.95.25.1. The Internet address 128.95.25.1 -- a unique identifier assigned to a specific computer connected to the Internet -- was affiliated with the University of Washington.

On February 27, 1997, Ontario police provided this information to the United States Customs Service attache in Canada. On March 11, 1997, the attache forwarded it to the Customs office in Seattle, Washington. Pursuant to a Grand Jury Subpoena issued in the Western District of Washington, the University of Washington informed Customs that the Internet address to which Evans sent the images was assigned to a computer within the University's Steven's Court housing facility. The University further advised Customs that this Internet address was associated with a particular Ethernet interface address (00C0F009C4DE) -- a unique identifier for a network card plugged into a computer. This Ethernet interface address was also associated with a second Internet address (128.95.25.203) which the University had assigned to Alexander Hay, an Electrical Engineering major. Both Inter-

2 FTP is a method of directly transferring files between two computers.

13393

net addresses were associated with a network port wired to the Steven's Court apartment occupied by Hay. University records showed that the computer in this apartment was configured sometimes to use the address 128.95.25.1 and other times to use the address 128.95.25.203.

The University also informed Customs agents of Hay's web site, which Customs Special Agent David Galante accessed on April 23, 1997. On it, Hay described extensive contacts with children, including teaching skiing to preschoolers, working as a preschool day camp counselor, babysitting, volunteering as a YMCA swim instructor for preschoolers, working with a four-year old autistic girl, and spending 400 hours as a volunteer in early primary school classrooms.

On May 5, 1997, Customs Special Agent Kristina Laider made an undercover telephone call to Hay at his apartment. The person who answered identified himself as Hay. Laider said she was conducting a computer usage survey and in

response to her questions, Hay stated that he owned a computer and kept it in his apartment; that he had an Ethernet card; that he currently used the University of Washington as an Internet Service Provider; and that he was the only user of his computer.

Galante made out a search warrant affidavit which stated that the 19 images sent by Evans were likely to be found in Hay's computer, described how traders and collectors of child pornography interact over the Internet, and explained that forensic experts could recover even deleted files. On May 28, 1997, a United States Magistrate Judge approved Galante's application and issued a warrant to search Hay's apartment and to seize Hay's computer hardware, software, records, instructions or documentation, and depictions of child pornography. Agents executing the warrant on May 29, 1997 at Hay's apartment seized his computer along with seven Zip cartridges labeled "Linux Backup," software, computer disks, and video tapes. One of the two hard drives on Hay's com-

13394

puter contained hundreds of computer graphics files depicting sexually explicit conduct involving minors, including "thumbnails" which enable the viewer to see multiple pictures simultaneously on the same screen, and an FTP log recording about 50 transactions with Evans.

After Hay was indicted for possessing and distributing child pornography, he moved to suppress this evidence for lack of probable cause to search and on the ground of staleness, but the district court denied the motion. The district court also denied Hay's motion to reconsider and to hold an evidentiary hearing in order to challenge the veracity of Galante's affidavit under Franks v. Delaware, 438 U.S. 154 (1978). The jury found Hay guilty of possession, receipt, reproduction and transportation of child pornography, and he has timely appealed.

II

A

Relying on United States v. Lacy, 119 F.3d 742 (9th Cir. 1997), and United States v. Weber, 923 F.2d 1338 (9th Cir. 1990), Hay contends that the government failed to establish probable cause because there was no evidence of a pattern of unlawful activity. Rather, in his view, the warrant affidavit merely reflected that Evans sent to an Internet address, sometimes linked to Hay's multi-user computer, a single transmission containing 19 images out of the 20,000 computerized images of child pornography found in Evans's computer system. Hay contends that the district court's ruling disregards the fact that pornographic materials can be received by "SPAM"³ as well as unintentionally by programs, such as the one Hay wrote, which, according to Hay, would automatically download files in bulk for later viewing. In addition, he notes, persons sending Internet transmissions using FTP can do so

³ "SPAM" is unsolicited junk e-mail.

13395

anonymously, further vitiating the basis for probable cause in this case.

In Weber, the defendant placed an order for four pictures of child pornography. Anticipating their delivery at his house, customs agents obtained a warrant to search for books, magazines, photographs, films, video tapes and undeveloped films depicting minors engaged in sexually explicit conduct based on an affidavit which stated the agent's belief that those items, as well as the four pictures which would arrive as a result of the controlled delivery, would be there. The boilerplate recited how the agent expected "child molesters," "pedophiles" and "child pornography collectors" to behave, but we found this was inadequate to support the application because there was no evidence in the affidavit indicating that Weber was any of those things. Id. at 1341. In these circumstances, we held that the affidavit was insufficient to establish probable cause that Weber would have anything other than the four pictures at his house.

In Lacy, Customs officials learned that child pornography from a Danish computer bulletin board system called BAMSE was being brought into the United States by computer, and

that an individual later identified as the defendant had downloaded six picture files containing computerized visual depictions known as GIFs. Based on a warrant affidavit which stated that Lacy downloaded at least two GIFs depicting minors engaged in sexual activity from BAMSE, a warrant was issued authorizing the search of Lacy's apartment and seizure of computer equipment and records, and documents relating to BAMSE. We held that this sufficed for probable cause to believe that Lacy actually received and possessed computerized visual depictions of child pornography.

Galante's affidavit is quite different from the affidavit we faulted in Weber. It contains a good deal of evidence from which the magistrate judge could conclude that the 19 files transmitted via FTP to Hay's Internet address would be found

13396

on Hay's computer system.⁴ Evans's log contained separate entries for each of the 19 file transfers and the transfers occurred at different times over a seven-minute period. The 19 files were not sent to Hay within or attached to an e-mail message; indeed, they did not go to Hay's e-mail address (ahay@dilbert.stc.housing.washington.edu) but to his Internet address (128.95.25.1) via FTP. FTP is a protocol for the direct transfer of files and has nothing to do with e-mail. Evans's files were downloaded directly into the "incoming " directory of Hay's computer. Galante's affidavit also recites information obtained from the University's records indicating that the computer located in Hay's apartment is sometimes configured to use the specific Internet address to which Evans transmitted, and from Hay himself that he is the exclusive user of the computer in his apartment. Further, there was evidence of Hay's extreme interest in young children as reflected in what Hay published on his home page. In light of these facts and the fact that Evans had been identified by Ontario police as an active trader of child pornography to the United States, the magistrate judge was entitled to infer that he and Hay had communicated prior to the 19 file transfers and that the transfers were neither unsolicited nor accidental. See United States v. Rowland, 145 F.3d 1194, 1205 (10th Cir. 1998) ("In making the probable cause determination, the issuing magistrate may draw reasonable inferences from the material provided in

the warrant application.").

Hay would have us infer otherwise for several reasons, one

4 We review for clear error whether the magistrate had a substantial basis for concluding probable cause existed, see United States v. Terry, 911 F.2d 272, 275 (9th Cir. 1990), and we accord "great deference" to the magistrate's determination of probable cause. United States v. Clark, 31 F.3d 831, 834 (9th Cir. 1994). The magistrate's responsibility in determining whether to issue a search warrant is "simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983).

13397

of which is that the search made of Evans's computer would surely have turned up evidence of prior communications had there been any. However, this supposes that the analysis of Evans's computer was comprehensive. Galante's affidavit provides no details about the nature and scope of the Evans's examination from which any inference one way or the other can reasonably be drawn. But the affidavit does provide sufficient information from which the magistrate judge could reasonably believe that there had to be prior communication because the 19 images were sent directly to Hay's computer by a known trader.

Beyond this, Hay argues that there was no evidence that he fell within a class of persons likely to collect and traffic in child pornography because the affidavit does not indicate that he was a child molester, pedophile, or collector of child pornography and sets forth no evidence that he solicited, sold or transmitted child pornography. In the same vein, Hay contends that Galante's affidavit did not establish a nexus between the crime and Hay's apartment because there was no evidence reflecting any specific illegal actions on Hay's part that took place in his apartment. However, these arguments misfocus the inquiry, which is whether there was reasonable cause to believe the 19 files from Evans's computer were located somewhere in Hay's computer, on electronic storage devices or on printouts, in his apartment. It is well-established

that a location can be searched for evidence of a crime even if there is no probable cause to arrest the person at the location. See Zurcher v. The Stanford Daily, 436 U.S. 547, 556 (1978) ("The critical element in a reasonable search is not that the owner of the property is suspected of crime but that there is reasonable cause to believe that specific 'things' to be searched for and seized are located on the property to which entry is sought."); United States v. Taketa, 923 F.2d 665, 674 (9th Cir. 1991) ("[T]he correct inquiry is whether there was reasonable cause to believe that evidence of . . . misconduct was located on the property that was searched."); United States v. Ocampo, 937 F.2d 485, 490 (9th Cir. 1991)

13398

("Probable cause exists when, considering the totality of the circumstances, there is a fair probability that contraband or evidence of a crime will be found in a particular place.") (citations and internal quotations omitted).

Hay also maintains that Galante's affidavit contained mostly generalized, boilerplate opinion testimony. Specifically, he faults language that individuals involved in possession and transportation of child pornography rarely, if ever, dispose of their sexually explicit material and that deleted computer files can likely be retrieved by computer experts. He also cites Galante's opinion that Hay was likely to possess more than the 19 images from Canada because "in most cases like this one, additional images have been found " and that the pornographic images "are rarely the first or last such images to be collected by the target." Based on Rowland, 145 F.3d at 1203-06, Hay argues that boilerplate language of this sort cannot rescue an affidavit devoid of evidence that he solicited or distributed child pornography and resting only on a bare inference that he must be a pedophile in possession of child pornography because of a single, seven-minute, six-month old transmission.

The "generalized" language in Galante's affidavit differs significantly from Rowland, where the defendant had given a post office box address for delivery of a videotape of child pornography that he ordered. The government obtained an anticipatory search warrant for Rowland's residence based

on an affidavit which described the investigator's training and experience in the area of child pornography but did not set out any facts suggesting there was reason to believe that Rowland would be likely to view or store such materials at his home rather than elsewhere. The court found the agent's general experience insufficient for probable cause in the absence of any evidence linking Rowland's home to the suspected criminal activity. Here, of course, the 19 files were not sent through the regular mail to Hay as the videotapes were in Rowland; they were directly transferred to Hay's computer. Also unlike

13399

Rowland, where the defendant used a post office box for receipt of pornographic materials, the affidavit here set forth evidence which linked the 19 files to Hay's apartment by tracing the IP address in Evans's FTP logs to the computer in Hay's apartment that Hay told government agents he used exclusively. Further, the boilerplate in Galante's affidavit provides context for Evans's transfer of 19 images to Hay's Internet address, and forms the basis upon which the magistrate judge could plausibly conclude that those files were still on the premises. It sets forth relevant background information about how child pornography is traded and distributed over the Internet: through use of chat rooms to establish contacts, followed by transmission or trading of images. It points out that the computer's ability to store images in digital form makes it an ideal repository for child pornography. The affidavit also explains that the computer has become one of the preferred methods of distribution of child pornographic materials and opines, based upon Galante's experience and that of colleagues, that searches and seizures of evidence from computers requires agents to seize all parts of a computer system to be processed later by a qualified computer expert. See United States v. Gil, 58 F.3d 1414, 1418 (9th Cir. 1995) ("[W]hen interpreting seemingly innocent conduct, the court issuing the warrant is entitled to rely on the training and experience of police officers."). In sum, the affidavit (including "boilerplate" based on the agents' experience), provides a substantial basis for the probable cause determination.

B

Hay additionally contends that the government's application, which took place six months after Evans transmitted the 19 images to Hay's computer, was too stale to justify the warrant. However, it follows from Lacy that information about the Evans's transmission was not stale. There, the defendant had downloaded child pornography ten months before the search warrant was sought and similarly argued staleness. Based on the affiant's explanation that collectors and distribu-

13400

tors of child pornography value their sexually explicitly material highly, rarely if ever dispose of it, and store it for long periods in a secure place, we concluded there was ample reason to believe the items sought were still in Lacy's apartment. As we stated, "[w]e are unwilling to assume that collectors of child pornography keep their materials indefinitely, but the nature of the crime, as set forth in this affidavit, provided good reason to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later." Lacy, 119 F.3d at 746 (internal quotations and citations omitted). The affidavit here makes similar statements, and also indicates that even if Hay had deleted the files, they could nevertheless be retrieved by a computer expert. As in Lacy, we conclude that the magistrate judge could well believe that the files sent by Evans would be present when the search was conducted.

In a related argument, Hay asserts that there must be a pattern of activity to infer long-term storage and to support a warrant in child pornography cases. For this he relies on our statement in Lacy to the effect that "[t]he information offered in support of the application for a search warrant is not stale if 'there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises.'" Lacy, 119 F.3d at 745-46 (quoting United States v. Gann, 732 F.2d 714, 722 (9th Cir. 1984)). While he is correct that a continuing pattern would support a warrant, so, too, do "other good reasons." Thus, the magistrate judge could properly authorize a search so long as there were good reasons to believe the 19 images were still in Hay's computer. As we have explained, there were.

C

Finally, Hay contends that the warrant was overbroad and lacked particularity because it authorized the government to search and seize Hay's entire computer system and virtually every document in Hay's possession without referencing child

13401

pornography or any particular offense conduct or being narrowed by specific acts, time frames or persons. Attachment A(1) to the application identifies (a) computer hardware, (b) computer software, (c) records stored in the form of electronic or magnetic coding or on computer media, (d) computer instructions, (e) printouts, photographs, video tapes or other visual depictions involving child pornography, and (f) records of the distribution of materials that depict child pornography. Attachment A(2) lists all records "involved with child pornography including, but not limited to" Evans and Hay. Although only subparagraphs (e) and (f) of Attachment A(1) specifically mention child pornography, the preface limits the scope of the search to "materials which constitute evidence of the commission of criminal offenses; or contraband, the fruits of crimes, or property designed or intended for use or which is or has been used as the means of committing criminal offenses, namely violations of 18 U.S.C. sections 2251 and 2252." These sections prohibit the sexual exploitation of children and certain activities relating to material involving the sexual exploitation of minors.

As was true in Lacy, "in this case no more specific description of the computer equipment sought was possible." Lacy, 119 F.3d at 746.⁵ The government knew that Evans had sent 19 images directly to Hay's computer, but had no way of

⁵ Descriptions in warrants must be specific enough to enable the person conducting the search to reasonably identify the things to be seized. See United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986). We consider the following factors in determining whether or not a warrant is overbroad:

- (1) whether probable cause exists to seize all items of a particular type described in the warrant;
- (2) whether the warrant sets out

objective standards by which executing officers can differentiate items subject to seizure from those which are not; and (3) whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant issued.

Id. at 963 (citations omitted).

13402

knowing where the images were stored. Further, the affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband. It also justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis. This, together with the magistrate judge's authorization to do so, makes inapposite United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), upon which Hay relies for its suggestion that magistrate judges should approve seizure of materials beyond those described in the warrant before wholesale removal occurs. In these circumstances, as we previously held in Lacy and as the Court of Appeals for the First Circuit has subsequently held in United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999), generic classification is acceptable.⁶

Hay compares the wholesale search and seizure of his apartment and computer system to searches and seizures condemned for overbreadth in United States v. Kow, 58 F.3d 423 (9th Cir. 1995), and Center Art Galleries-Hawaii, Inc. v. United States, 875 F.2d 747 (9th Cir. 1989) overruled on other grounds, J.B. Manning Corp. v. United States, 86 F.3d 926, 927 (9th Cir. 1996), but the same argument was rejected in Lacy. Both Kow and Center Art are distinguishable in any event. In Kow, the alleged crime was tax fraud and the warrant authorizing "the seizure of virtually every document and

⁶ Upham rejected a similar attack on the generic nature of the warrant application in a case which also involved the computer transmission of child pornography, observing:

As a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the nar-

rowest definable search and seizure reasonably likely to obtain the images. A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.

168 F.3d at 535.

13403

computer file" at a video distributing company was unconstitutionally broad and generic because there was no limit on which documents could be seized or how they related to the criminal activity at issue. Center Art Galleries involved an investigation of mail and wire fraud in connection with the sale of a forged Salvador Dali artwork. The warrant was overbroad because it allowed virtually unrestricted seizure of items without describing the specific crimes suspected. See also United States v. Cardwell, 680 F.2d 75 (9th Cir. 1982) (warrant invalid because it failed to describe criminal activity under investigation). By contrast, in this case, the application did not ask for, and the warrant did not authorize, seizure of every document, but of child pornography which is a sufficiently specific definition to focus the search. ⁷

III

Hay submits that he was entitled to a hearing under Franks v. Delaware, 438 U.S. 154 (1978), because the warrant affidavit misled the magistrate judge into believing that Hay owned the sole computer tied to the 128.95.25.1 Internet Protocol address to which Evans sent the child pornography. ⁸ The warrant affidavit provided that the transmission had to have been made solely to Hay's computer because the 128.95.25.1 Internet address was linked to the unique identifier of the Ethernet interface address (00C0F009C4DE) for Hay's computer. He proposed to show that the government intentionally or reck-

⁷ We decline to consider Hay's argument that execution of the warrant was overbroad as it was not raised in the district court. See United States v. Robertson, 52 F.3d 789, 791 (9th Cir. 1994). Regardless, so far as appears, nothing that was seized or searched which arguably exceeded the

scope of the warrant was used. No plain error would, therefore, have occurred.

8 "In order to be granted a Franks hearing, the defendant must make a substantial preliminary showing that: 1) the affidavit contains intentionally or recklessly false statements, and 2) the affidavit cannot support a finding of probable cause without the allegedly false information." United States v. Valencia, 24 F.3d 1106, 1109 (9th Cir. 1994).

13404

lessly failed to reveal that University of Washington ARP cache data computer logs reflected that a second computer with a different Ethernet address (00A024AF91) frequently used the same 128.95.25.1 address. However, the warrant application was based on information provided by the University pursuant to a grand jury subpoena, none of which indicated that the IP address 128.95.25.1 was linked to any other computer. As Hay failed to make any showing that Galante knew of the second Ethernet interface address at the time of making out the affidavit, or had any basis for believing the information furnished by the University and included in the affidavit was not true, a Franks hearing was not required.

IV

Hay seeks reversal of his conviction on the ground that the district court improperly allowed the jury to view three exhibits of photographic depictions of child pornography even though he had stipulated that they constituted child pornography transmitted in interstate commerce. Hay had moved in limine to exclude all thirty-four exhibits that depicted child pornography under Federal Rules of Evidence 403(b). The district court ruled that no images of child pornography would be shown to the jury except upon request, and none was published during the trial. However, during deliberations the jury requested three specific exhibits. One was an image that Hay sent to someone while engaged in an Internet chat on March 16, 1997 that showed Hay (not a hacker) was interested in child pornography and involved in its distribution. Another was the packet of recovered child pornography files from the partition of Hay's hard drive that he backed up onto the seven encrypted Zip cartridges; this exhibit also showed that Hay

(rather than a hacker) distributed child pornography. The third exhibit was a reconstruction of a page from Hay's web site based on the contents of his own web browser cache, which showed Hay using his browser to access his system.

13405

Hay contends that United States v. Merino-Balderrama, 146 F.3d 758 (9th Cir. 1998), mandates a new trial. In Merino-Balderrama, child pornography films that were in a briefcase in the defendant's car were played for the jury. There was no evidence that the defendant had seen the films. We reversed because the box covers had still photographs which were more probative of the defendant's knowledge that they contained pornographic material than the films, yet were far less inflammatory. Unlike Merino-Balderrama, there was evidence that Hay had seen the images of child pornography which he was charged with possessing, based on the thumbnail images he created when he viewed them on his computer screen as well as the existence of many of the images on his own FTP and web sites. Further, the nature of the images was relevant in light of Hay's claims at trial that he had tried to delete images he found on his system and that a hacker had taken over his computer. Finally, the particular three exhibits that were shown to the jury reflected Hay's personal involvement. Given Hay's defenses, we cannot say that allowing the jury to view three of the thirty-four exhibits was unduly prejudicial.

V

After briefing was completed, Hay submitted papers suggesting that his conviction might be infirm in light of Free Speech Coalition v. Reno, 198 F.3d 1083 (9th Cir. 1999), where we held that the First Amendment prohibits Congress from enacting a statute that makes criminal the generation of images of fictitious children engaged in imaginary but explicit sexual conduct. Subsections (B) and (D) of 18 U.S.C. § 2256(8) were at issue in Free Speech. Section 2256(8)(B) bans sexually explicit depictions that appear to be of minors, and § 2256(8)(D) bans visual depictions that are "advertised, promoted, presented, described or distributed in such a manner that conveys the impression" that they contain sexually

explicit depictions of minors. We struck these subsections because language that criminalizes material that "appears to

13406

be a minor" and "conveys the impression" that a minor is engaged in explicit sexual activity is unconstitutionally vague and overbroad.

Hay never challenged the indictment or the instructions on this ground. Indeed, he stipulated that the computer graphics files recovered from his system involved children under the age of eighteen and the stipulation listed the age range of each child in each of the exhibits. Counsel conceded that the material was child pornography. Even assuming the issue is not waived, only one of the counts was charged under § 2256(8) and it does not focus on the two phrases at issue in Free Speech. To the contrary, the jury was specifically instructed that the term "child pornography" means any visual depiction of sexually explicit conduct where "the production" involves the "use of a minor [defined as "any person under the age of eighteen years"] engaging in sexually explicit conduct" and "such visual depiction is of [a person under the age of eighteen years] engaging in sexually explicit conduct." A production using a child is very different from morphing, and Hay does not suggest how there could be anything unconstitutional about this definition. We see no error, plain or otherwise.

AFFIRMED.

13407